

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN**

ECOLAB Inc., and NALCO COMPANY,
LLC d/b/a Nalco Water, an Ecolab Company
and/or Nalco Water,

Plaintiffs,

v.

JESSICA GRAILER,

Defendant.

No. 3:23-cv-00102

**FIRST AMENDED VERIFIED COMPLAINT FOR INJUNCTIVE RELIEF, DAMAGES
AND OTHER RELIEF**

Plaintiffs Ecolab Inc. (“Ecolab”) and Nalco Company LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water (“Nalco”) (hereafter Ecolab and Nalco may be collectively referred to as “Company” or “Plaintiffs”), through undersigned counsel, bring this Amended Verified Complaint for a Preliminary Injunctive Relief, a Permanent Injunction, Damages and Other Relief against Defendant Jessica Grailer, hereby alleging the following causes of actions: Violation of the Defend Trade Secrets Act, Violation of the Wisconsin Trade Secrets Act, Violation of the Computer Fraud and Abuse Act, and Breach of Contract.

NATURE OF ACTION

1. This action is brought against Plaintiffs’ former Account Manager who after resigning from the Company to join a competitor, accessed Plaintiffs’ computer network and misappropriated numerous documents containing Plaintiffs’ confidential and trade secret information. Plaintiffs seek damages and injunctive relief enjoining Defendant from further misappropriating Plaintiffs’ confidential and trade secretion information.

2. Just days after giving Plaintiffs notice of her voluntary resignation to join a direct competitor, and after being instructed that she was no longer to do any work further for Plaintiffs,

was to return all property, and expressly advised “not to steal” Plaintiffs’ information, Defendant accessed and downloaded hundreds of company documents containing company confidential and trade secret information. Defendant, days after returning her company assigned laptop, accessed Plaintiffs’ computer network through the cloud and accessed numerous documents containing Plaintiffs’ confidential and trade secret information. The information misappropriated by Defendant Grailer was extremely valuable to Plaintiffs as it would be to any employer similarly engaged in the highly competitive business of monitoring and controlling performance of industrial water treatment systems. Defendant illegally accessed, downloaded this information, and erased other Company data, despite signing contractual obligations prohibiting her from doing so and despite being expressly instructed that she was not to steal Plaintiffs’ business information.

3. In addition to economic and other damages, this action seeks temporary, preliminary and permanent injunctive relief enjoining Defendant and those acting in concert with her from continuing to possess, utilize, and/or disclose Plaintiffs’ confidential information and trade secrets and requiring Defendant to preserve and return all wrongfully retained Company property.

PARTIES

4. Ecolab, Inc. (“Ecolab”) is a Delaware corporation with its principal place of business in the State of Minnesota. Ecolab is registered to do business and regularly conducts business in the State of Wisconsin and maintains a registered agent in the State of Wisconsin at 301 S. Bedford St., Ste. 1, Madison, WI 53703.

5. Nalco Company, LLC (“Nalco”) is a Delaware limited liability company with its principal place of business in the State of Illinois. Nalco is registered to do business and regularly conducts business in the State of Wisconsin and maintains a registered agent in the State of Wisconsin at 301 S. Bedford Street, Ste. 1, Madison, WI 53703. Nalco does business under the

trade names “Nalco Water, an Ecolab Company” and “Nalco Water.” Nalco is a subsidiary of Ecolab.

6. Defendant Jessica Grailer resides in and is a citizen of the State of Wisconsin.

JURISDICTION AND VENUE

7. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because Plaintiffs are asserting claims for trade secret misappropriation under the federal Defend Trade Secrets Act, 18 U.S.C. § 1836, *et seq*, and the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

8. The Court has supplemental jurisdiction over Plaintiffs’ remaining causes of action under 28 U.S.C. § 1367, which states “the district courts shall have supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy[.]”

9. This Court has personal jurisdiction over Defendant Grailer under Federal Rule of Civil Procedure 4 as Defendant Grailer resides and is a citizen of the State of Wisconsin.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant Grailer resides in the Western District of Wisconsin and the events giving rise to Plaintiff’s claims against Defendant Grailer substantially occurred within the District.

FACTUAL ALLEGATIONS

The Company’s Business, Confidential Information, and Trade Secrets

11. Ecolab and its subsidiary Nalco are global leaders in industrial process and water treatment services, providing high quality water treatment management services to clients in such industries as food preparation, pulp and paper, agriculture, manufacturing, refining, mining, power production, healthcare, pharmaceutical, and high tech. They provide a broad spectrum of products

and services to businesses throughout the United States including the State of Wisconsin, where they maintain a robust business.

12. Management of industrial water treatment systems is a highly competitive business, and Ecolab and Nalco's clients, partners, and vendors are critical to their success in the growing and competitive market.

13. Ecolab and Nalco partner with companies across a wide range of industries and develop solutions for each client's specific water treatment needs and business goals. This specialized information pertaining to each client is proprietary in nature and would be highly valuable to Ecolab and Nalco's competitors.

14. Ecolab and Nalco have invested considerable sums of money in developing products, equipment, training programs, sales programs, technical service programs, and account records for the proper servicing of their customers.

15. Ecolab and Nalco have developed and maintain a substantial amount of trade secret and confidential and proprietary information, including but not limited to: business plans; pricing, marketing and distribution strategies; product, branding, packaging and advertising development; brand portfolio strategies; vendor/supplier relationships; global supply chain; client lists, preferences, and plans; the specific types of services performed for customers and clients; the type of equipment ordered or installed for customers or clients; the prices paid by each customer; business partner relationships and agreements; discount structures; channel development; product formulas; technical specifications, and intellectual property ("Trade Secret and Confidential Information").

16. Ecolab and Nalco's Trade Secret and Confidential Information was developed over many years, with a substantial investment of labor, skill, money, and knowledge gained from

experiences with clients, partners, technical experts, vendors, as well as other outside entities and agencies, among others.

17. Ecolab and Nalco's Trade Secret and Confidential Information is highly valuable, not generally known outside of the Company, and would be of significant value to the Company's competitors if wrongfully disclosed to such entities. Ecolab and Nalco derive a competitive advantage and independent economic value, both actual and potential, from its Trade Secret and Confidential Information, because the Trade Secret and Confidential Information is not generally known to the public or to others who can obtain economic value from its disclosure or use.

18. In order to protect their Trade Secret and Confidential Information, Ecolab and Nalco, among other things, require employees to execute agreements tailored to protect their valuable company assets, including by: (1) prohibiting employees from transferring or storing Company information onto any device or storage medium (physical or virtual) not provided or authorized in writing by the Company; (2) prohibiting departing employees from wiping, deleting or transferring any Company data from any electronic devices before returning such devices to the Company; (3) requiring employees who separate from the Company to return all Company property, data, business information, phones, computers, and electronic devices; and (4) requiring employees to acknowledge and agree that employees have no right to privacy regarding any Company property and as such that Company has the right to conduct forensic examination(s) of any Company computers and/or electronic devices issued to employees or authorized for employee use for Company business.

19. Ecolab and Nalco also strictly require the use of computer passwords, limit access to Trade Secret and Confidential Information only to employees that need the information to perform their duties for the Company, maintain confidentiality policies in employee handbooks, maintain electronic communication and code of conduct policies regarding confidentiality, and

stress the importance of maintaining confidentiality to protect Trade Secret and Confidential Information.

20. Ecolab and Nalco also use a secure computer network to store and maintain their proprietary, Trade Secret and Confidential Information.

Defendant's Employment and Acquisition of Trade Secret and Confidential Information

21. Defendant Grailer was employed by Nalco as an Account Manager, based in Verona, Wisconsin, where she focused on sales and service of Plaintiffs' customers with water treatment needs, primarily those needing treatment services involving ethanol.

22. As Plaintiffs' Account Manager, Defendant managed industrial and institutional accounts in the State of Wisconsin, in eastern Minnesota, and northern Illinois. This included managing client water treatment processes, such as reviewing and analyzing technical chemical treatment data, reviewing operations and procedures, as well as managing and troubleshooting chemical formulations and reformulations. Defendant was responsible for maintaining and servicing the Company's accounts and soliciting new business accounts through resources provided by the Company.

23. Defendant provided services to, supported, and/or serviced clients of the Company.

24. In order to perform her duties, Defendant was privy and given access to certain Company Trade Secret and Confidential Information.

Defendant Agrees to Hold the Company's Trade Secret and Confidential Information in a Fiduciary Capacity

25. As a condition of her employment, Defendant executed an Employee Sales, Service, Marketing & Inventions Agreement (the "Employee Agreement"), attached hereto as **Exhibit A**.

26. Defendant and an Ecolab representative executed the Employee Agreement, which also provides protections to Ecolab's "parent companies, sister companies, and subsidiaries" such as Nalco.

27. As part of the Employee Agreement, Defendant acknowledged that by the nature of her role, she would "acquire knowledge of Company's Trade Secrets and its Confidential Information, which may include without limitation, information regarding present and future operations, customers and suppliers, pricing, business strategies, business methods, and employees (including the particular skills, talents and abilities of those employees)." See **Exhibit A**, ¶ 2.

28. The Employee Agreement defines Trade Secrets as:

[I]nformation pertaining to Company including, but not limited to, a formula, pattern, compilation, program, device, method, technique or process, financial data, financial plans, product plans, a list of actual or potential customers or suppliers, pricing information, information about customer contacts, requirements or purchasing patterns, or the identities of or contact information for actual or potential customers or suppliers of Company that both:

(a) derives economic value, actual or potential from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(b) is the subject of efforts by Company that are reasonable under the circumstances to maintain its secrecy.

See **Exhibit A**, ¶ 2.

29. With regard to Trade Secrets, Defendant agreed to hold such information "in a fiduciary capacity for the benefit of Company" and not to "directly or indirectly, use or disclose" any such information that she "may have acquired during the term of Employee's employment with Company for so long as such information remains a Trade Secret." See **Exhibit A**, ¶ 2.

30. The Employee Agreement defines Confidential Information as:

Company's confidential data or information which is valuable to Company but substantially inaccessible to the public and to competitors of Company, including, without limitation, business information, financial data, product information, the identities and contact information of actual or potential customers or suppliers, pricing information, and other information of a proprietary nature regarding the Company's business operations, excluding Trade Secrets. Notwithstanding the

foregoing, the term “Confidential Information” shall not include information that Employee can establish by competent proof: (i) was generally known to or accessible by the public at the time Company disclosed the information to Employee; (ii) became generally known to or accessible by the public after disclosure by Company through no act or omission by Employee; or (iii) was disclosed to Employee, after the Employee’s termination of employment with the Company, by a third party having a bona fide right both to possess the information and to disclose the information to Employee, provided such third party is not subject to an obligation of confidentiality with respect to such information.

See **Exhibit A**, ¶ 2.

31. With regard to Confidential Information, Defendant agreed “that while employed with the Company and for a period of three (3) years after termination of Employee’s employment with Company” that she would hold such information “in a fiduciary capacity for the benefit of Company” and would not “directly or indirectly, use or disclose” any such information “that Employee may have acquired (whether or not developed or compiled by Employee and whether or not Employee was authorized to have access to such Confidential Information) during the term of, in the course of, or as a result of Employee’s employment by Company.” See **Exhibit A**, ¶ 2.

32. The Employee Agreement also required that, upon termination of employment or Company request, Defendant would:

[R]eturn in good order all Company property and information in the Employee’s possession, custody or control. Upon termination, Employee shall return all Company data, business information, credit cards, keys, automobiles and any other Company property in her possession. Employee shall not erase or delete any Company data from Company phones or computer or other electronic devices except as may be necessary in the regular course of conducting business for the Company. For example, it would be a violation of this provision for Employee to accept a position with another entity and/or give notice of Employee’s resignation and then delete and/or erase Company data from Employee’s Company assigned phone and/or computer device.

See **Exhibit A**, ¶ 11.

Defendant’s Voluntary Resignation and Subsequent Misappropriation of the Company’s Highly Confidential and Trade-Secret Information

33. On January 8, 2023, Defendant Grailer advised Plaintiffs that she was voluntarily resigning to join Plaintiff’s direct competitor, ChemTreat.

34. Defendant's supervisor advised her that she was done and relieved of all duties on behalf of Plaintiffs and Defendant was instructed not to "steal" the Company's information.

35. On January 11, 2023, Defendant returned her company assigned laptop to Plaintiffs.

36. On or about January 15, 2023, after Defendant Grailer was separated from employment, and after she had returned her Company assigned laptop computer, she accessed the Plaintiffs' computer network through the cloud to access, view, and download numerous documents containing Plaintiffs' confidential and trade secret information.

37. On January 15, 2023, Defendant Grailer, without authorization, accessed Plaintiffs' computer network and documents therein containing confidential chemical formulas, customer specific information, and personnel information.

38. The Company has since retained a forensic expert who has only just begun to uncover the full extent of Defendant's misappropriation of Company Trade Secret and Confidential Information. So far, the Company has uncovered information demonstrating that after her termination from employment that Defendant Grailer accessed numerous documents and files belonging to Plaintiffs, including files containing highly confidential and trade secret information concerning the Company's business and customers.

39. The forensic investigation revealed that on January 8, 2023, after informing Plaintiffs of her resignation and after being told by Plaintiff to cease performing any and all work, Defendant attached an external USB drive (the "Emtec USB Drive") to her company-issued laptop at 9:39 p.m. Central.

40. The forensic investigation revealed that Defendant accessed multiple files from the Emtec USB Drive containing highly sensitive and confidential information.

41. Specifically, Defendant downloaded and exfiltrated 159 files on January 8, 2023, at 7:20 p.m. Central and 2 files at 8:48 p.m. Central.

42. Defendant also downloaded and exfiltrated one PDF document on January 8, 2023 at 8:56 p.m. Central, and 128 Excel documents on January 8, 2023 at 7:33 p.m. Central and 9:04 p.m. Central.

43. Furthermore, Defendant downloaded 43 pictures of Ecolab, Nalco, or customer equipment on January 8, 2023 at 9:11 p.m. Central.

44. The forensic investigation also revealed that Defendant downloaded 66 email attachments from her Ecolab Outlook email account on January 8, 2023 between 3:46 a.m. Central and 8:50 p.m. Central.

45. Plaintiff did not authorize or knowingly permit Defendant to access, download, e-mail, print or otherwise appropriate any of Plaintiffs' information and files that she exfiltrated on and after January 8, 2023. Many of the files Defendant illegally accessed and downloaded are highly sensitive, confidential and constitute the Company's Trade Secret and Confidential Information.

46. The forensic investigation revealed that on January 14, 2023 at 12:52 a.m. Central, Defendant attempted to access her Ecolab OneDrive account using an undisclosed iPhone 12 Mini. The forensic investigation revealed that later on January 14, 2023, Defendant was successful in accessing her Ecolab OneDrive account.

47. The forensic examiner's investigation confirmed that on January 15, 2023 at 1:01 p.m. Central, several days after Plaintiff's separation from employment, Defendant unlawfully accessed her Ecolab OneDrive account and infiltrated at least 20 of Plaintiffs' files, some of which contain highly confidential and trade secret information concerning the Company's business and customers.

48. Defendant improperly deleted Company business information, including improperly deleting Company data from her company assigned iPhone.

49. The Company's Trade Secret and Confidential Information misappropriated by Defendant includes internal product bulletins that contain proprietary product constituents, proprietary product dosage and feeding information, and critical success factors. Defendant also misappropriated personnel information related to Plaintiffs' employees engaged in the Food and Beverage sector. Defendant also misappropriated detailed customer service reports, sales quotes, key performance indicators for customers, detailed pricing information, field service pricing, wastewater trial calculations, return on investment information, chemical formations, detailed product information, information regarding developing technology such as Evaporation Treatment Technology, boiler calculations, customer specific processes and calculations, dosage calculations, and Nalco's proprietary Light N.A. Pricing tool. Further concerning is the fact that some of the confidential information that Defendant misappropriated was not related to the work Defendant performed for Plaintiff but rather it dealt with a separate area of Plaintiffs' business.

50. Upon review of the two Company phones that Defendant used and returned to Plaintiffs, one phone apparently had not made a phone call since October 22, 2020, and had not sent a text message since August 19, 2020, despite the fact that Defendant continued to work for the Company through January 11, 2023. A second Company phone returned by Defendant was factory reset prior to being returned to the Company, thus destroying all of the phone's contents. Both phones do not show any activity in the last two years.

51. Additional information obtained from the forensic investigation revealed that Defendant had actually accepted employment with ChemTreat back in mid to late December 2022.

52. For example, the forensic investigation revealed that, on December 15, 2022, Defendant accessed and downloaded a file titled "Offer Letter Document 2022 12 14.pdf." The file "Offer Letter Document 2022 12 14.pdf" included a tentative start date for Jessica Grailer at ChemTreat of January 3, 2023.

53. The forensic investigation also revealed that on December 15, 2022, Defendant downloaded a file titled “Jessica Grailer (Pay Plan).pdf.” On December 15, 2022 at 9:30 p.m. Central, Defendant saved a file titled “Jessica Grailer (Pay Plan) (1).pdf” containing her signature and a start date of “TBD.”

54. The forensic investigation further revealed that on December 21, 2022 at 8:48 a.m. Central, Defendant received an email with the subject “Signature requested on ChemTreat New Hire Policies.” On December 21, 2022 at 8:57 a.m. Central, Defendant received an email with the subject “You signed: ChemTreat New Hire Policies.”

55. The Company is entitled to temporary, preliminary, and permanent injunctive relief preventing any actual or threatened misappropriation and misuse of its Trade Secret and Confidential Information by Defendant and/or her agents, and other persons who are in active concert or participation with them (collectively, “Covered Persons”).

56. This injunctive relief should include, without limitation, an Order prohibiting the Covered Persons from using or disclosing any of the Company’s Trade Secret and Confidential Information in any manner.

57. Further, the injunctive relief should include an Order requiring the Covered Persons to return to the Company, and not retain in their possession, custody, or control, any and all Trade Secret and Confidential Information of the Company, and to certify under oath that all Trade Secret and Confidential Information has been returned.

58. The Company has a substantial likelihood of prevailing on the merits of its claims.

59. Unless the Covered Persons are enjoined from the conduct described herein, there is a substantial threat that the Company will continue to suffer irreparable harm, including loss and misuse of its Trade Secret and Confidential Information, goodwill, and financial losses that presently are not calculable.

60. The irreparable harm that the Company will suffer if injunctive relief is denied outweighs the potential harm (if any) to Defendant if injunctive relief is granted.

61. Granting the requested injunctive relief will not disserve the public interest.

62. The Company has no adequate remedy at law.

63. Consequently, the Company is entitled to injunctive relief as set forth herein.

COUNT I

Violation of the Defend Trade Secrets Act (18 U.S.C. § 1831 *et seq.*)

64. Plaintiffs incorporate the preceding paragraphs as though set forth herein.

65. Ecolab and Nalco have developed trade secret information including, but not limited to, technical data, formulas, patterns, compilations, ratios, programs, methods, techniques, processes, know-how and plans that derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from their disclosure or use.

66. The information, documents, and materials stolen and misappropriated by Defendant constitute trade secrets within the meaning of, and subject to protection under, the Defend Trade Secrets Act (“DTSA”), 18 U.S.C. § 1831 *et seq.*

67. Ecolab and Nalco regularly transact business throughout the United States, including in person and by phone, internet, and mail, and the Company’s trade secrets relate to this business and are used in interstate commerce.

68. Defendant acquired the Company’s trade secrets by improper means, including but not limited to knowingly accessing, downloading, and using this information in violation of her contractual duties owed to the Company.

69. The information contained in these documents is valuable because it is not generally known or readily accessible, through proper means, to others who can profit from its

use. The Company has spent significant sums, in terms of both financial and human resources, to develop and maintain this information, which would be of great value to any competitor.

70. Ecolab and Nalco take, and at all times here relevant, have taken reasonable measures to maintain the confidential and secret nature of this information. Those steps include restricting availability of confidential information to key employees, requiring key employees (like Defendant) to execute agreements with confidentiality provisions and restrictive covenants, physical security measures to protect against the disclosure of sensitive materials to third parties, and IT security efforts.

71. By accessing the Company's computer network without authorization, and downloading trade secret information, Defendant has committed both an actual and threatened misappropriation and misuse of the Company's trade secret information in violation of the DTSA.

72. Upon information and belief, and as the Company expects to establish on further investigation and discovery, Defendant has improperly retained, used, and/or disclosed (and continues to retain, use, and/or disclose) confidential business information and strategies and trade secrets contained in the documents and information she took or disclosed from the Company without authorization and in breach of her contractual duties owed to the Company in order to compete against the Company.

73. Defendant engaged in this conduct despite acquiring this information without authorization.

74. Upon information and belief, Defendant engaged in this misconduct at a time she was no longer employed with the Company and after she was instructed not to access the Company's computer database.

75. As a direct and proximate result of Defendant's actual and threatened misappropriation of trade secrets, the Company has suffered irreparable harm and will continue to

suffer irreparable harm that cannot be adequately remedied at law unless Defendant is enjoined from engaging in any further acts of misappropriation and from continued possession in any form of trade secret information belonging to the Company.

76. To the extent that Defendant has already provided the Company's trade secrets or other confidential information to third parties, those parties should also be ordered to return and/or destroy that information.

77. As a direct and proximate result of Defendant's misappropriation, the Company has suffered and continues to suffer damages and irreparable harm, and is entitled to all damages, attorneys' fees, costs and remedies permitted under the DTSA. Each of the acts of misappropriation was done willfully and maliciously by Defendant to unfairly compete against the Company and benefit herself and third parties, thereby entitling Plaintiffs to exemplary damages to be proved at trial.

COUNT II

Violation of the Wisconsin Trade Secrets Act (Wisc. Stat. Ann. § 137.90 *et seq.*)

78. Plaintiffs incorporate the preceding paragraphs as though set forth herein.

79. Ecolab and Nalco have developed trade secret information including, but not limited to, technical data, formulas, patterns, compilations, ratios, programs, methods, techniques, processes, know-how and plans that derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from their disclosure or use.

80. The information, documents, and materials stolen and misappropriated by Defendant constitute trade secrets within the meaning of, and subject to protection under, the Wisconsin Trade Secrets Act (Wisc. Stat. Ann. § 137.90 *et seq.*)

81. Ecolab and Nalco regularly transact business throughout the United States, including in person and by phone, internet, and mail, and their trade secrets relate to this business and are used in interstate commerce.

82. Defendant acquired Ecolab and Nalco's trade secrets by improper means, including but not limited to knowingly accessing, downloading, and using this information in violation of her contractual and legal duties owed to the Company.

83. The information contained in these documents is valuable because it is not generally known or readily accessible, through proper means, to others who can profit from its use. Ecolab and Nalco have spent significant sums, in terms of both financial and human resources, to develop and maintain this information, which would be of great value to any competitor.

84. Ecolab and Nalco take, and at all times here relevant, have taken reasonable measures to maintain the confidential and secret nature of this information. Those steps include restricting availability of confidential information to key employees, requiring key employees (like Defendant) to execute agreements with confidentiality provisions and restrictive covenants, physical security measures to protect against the disclosure of sensitive materials to third parties, and IT security efforts.

85. By accessing the Company's computer network without authorization and downloading trade secret information and accessing and downloading trade secret information prior to returning her company-issued laptop, Defendant has committed both an actual and threatened misappropriation and misuse of the Company's trade secret information in violation of the ATSA.

86. Upon information and belief, and as Plaintiffs expect to establish on further investigation and discovery, Defendant has improperly retained, used, and/or disclosed (and continues to retain, use, and/or disclose) confidential business information and strategies and trade

secrets contained in the documents and information she took or disclosed from the Company without authorization and in breach of her contractual duties owed to the Company in order to compete against the Company.

87. Defendant engaged in this conduct despite acquiring this information without authorization.

88. Upon information and belief, Defendant engaged in this misconduct at a time she was no longer employed by Nalco and after she was expressly instructed not to access the Company's information and had been separated by the Company.

89. As a direct and proximate result of Defendant's actual and threatened misappropriation of trade secrets, the Company has suffered irreparable harm and will continue to suffer irreparable harm that cannot be adequately remedied at law unless Defendant is enjoined from engaging in any further acts of misappropriation and from continued possession in any form of trade secret information belonging to the Company.

90. To the extent that Defendant has already provided the Company's trade secrets or other confidential information to third parties, those parties should also be ordered to return and/or destroy that information.

91. As a direct and proximate result of Defendant's misappropriation, the Company has suffered and continues to suffer damages and irreparable harm, and is entitled to all damages, attorneys' fees, costs and remedies permitted under the ATSA. Each of the acts of misappropriation was done willfully and maliciously by Defendant to unfairly compete against the Company and benefit herself and third parties, thereby entitling Plaintiffs to exemplary damages to be proved at trial.

COUNT III
Violation of Computer Fraud and Abuse Act (18 U.S.C. § 1030 et seq.)

92. Plaintiffs incorporate the preceding paragraphs as though set forth herein.

93. The federal Computer Fraud and Abuse Act (“CFAA”) provides, “[w]hoever. . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains. . . information from any protected computer. . . shall be punished as provided in subsection (c) of this section.” 18 U.S.C.A. § 1030(a)(2)(C). The Act provides that a person who accesses a computer with authorization, nevertheless “exceeds authorized access” if she uses her access “to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter.” 18 U.S.C.A. § 1030(e)(6).

94. The Act provides that “[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C.A. § 1030(g). A civil claim under the Act may be brought by any person who has suffered or would have suffered damages, loss or injury as described in Sections (a)(5)(B)(i)-(v) of the Act. A “loss” is defined in the Act as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C.A. § 1030(e)(11).

95. Section (a)(4) of the Act likewise prohibits actions whereby a person “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value. . . .” 18 U.S.C.A. § 1030(a)(4).

96. Defendant’s wrongful access of the Company computer network and database without authorization, at a time she was no longer employed by Nalco, and after expressly being

instructed that she was no longer authorized to access the Company's computer devices or computer network, constitutes a violation of the Computer Fraud and Abuse Act.

97. As a result of Defendant's violation of the Computer Fraud Act, Plaintiffs have suffered and continue to suffer loss and damage to the integrity of data, computer systems and loss of confidential information and trade secrets, resulting in damages far in excess of \$5,000.00 and absent injunctive relief will continue to suffer irreparable harm and damages.

COUNT IV
Breach of Contract – Employee Agreement

98. Plaintiffs incorporate the preceding paragraphs as though set forth herein.

99. The Employee Agreement is a valid and enforceable contract executed by Defendant on or about April 20, 2021.

100. Defendant's compliance with the Employee Agreement and the covenants therein were conditions precedent to her employment or continued employment.

101. Defendant breached and is continuing to breach her contractual promise not to, directly or indirectly, misuse or improperly disclose the Company's Trade Secrets for so long as such information remains a Trade Secret.

102. Defendant breached and is continuing to breach her contractual promise not to, directly or indirectly, misuse or improperly disclose the Company's Confidential Information for a period of three (3) years after this voluntary or involuntary termination from employment.

103. Defendant breached and is continuing to breach her contractual promise to promptly return all Company property and information, including Trade Secrets and Confidential Information to Company's possession.

104. Defendant impermissibly possesses and continues to possess the Company's Trade Secret and Confidential Information in furtherance of Defendant's efforts to unfairly compete. In doing so, Defendant has violated her obligation to hold this information in a fiduciary capacity and

to refrain from using this information except as necessary to perform her duties for the Company or as otherwise authorized by the Company.

105. Defendant breached her contractual promise not to not erase or delete any Company data from Company phones or computer or other electronic devices when she factory reset a Company phone.

106. The Company has already been severely injured by Defendant's improper and prohibited actions. If Defendant is not enjoined from continuing to breach her contractual duties, the Company will continue to be irreparably injured.

107. As a result of Defendant's breach of her contractual obligations, the Company has been damaged, and will continue to be damaged, in an amount to be proven at trial.

JURY DEMAND

The Company respectfully demands a trial by jury on all counts.

PRAYER FOR RELIEF

WHEREFORE, by virtue of the foregoing acts complained of, Plaintiffs respectfully requests that this Honorable Court enter one or more orders granting it the following relief:

A. A temporary restraining order, preliminary injunction, and a permanent injunction requiring Defendant (and any persons acting in concert with him or on her behalf) ordering that:

1) Defendant, her agents, servants, employees, representatives, and attorneys, and other persons who are in active concert or participation with any of the foregoing (collectively, "Covered Persons") are ordered, restrained and enjoined as follows:

i. Directly or indirectly, disclosing or making any use of any Trade Secret and Confidential Information of Ecolab and Nalco;

- ii. Provide a full and complete accounting of all electronic devices, email accounts, cloud-storage accounts, and other devices/accounts that Grailer had access to and that any of the information that Grailer improperly downloaded and copied may have been downloaded to or accessed as stated in the Complaint;
 - iii. Take all necessary steps to maintain and preserve all potentially relevant evidence regarding the allegations in the Complaint, including, but not limited to, all indicia and potential evidence relating Grailer's misappropriation of Ecolab's trade secrets and confidential/proprietary information and her and others potential access of that same information by any and all electronic devices, email accounts, including internet e-mail accounts, cloud-storage based accounts, and the like within its possession, custody or control;
 - iv. Make available for inspection and imaging all computers, external storage devices, mobile devices, and all personal Cloud and email accounts including internet-based e-mail accounts in Grailer's possession and/or control, to determine the full extent of Defendant Grailer's access, possession, retention, and use of Ecolab's confidential information or trade secrets.
- 2) the Covered Persons return to Plaintiffs any Trade Secret and Confidential Information that is in their possession, custody, or control (including but not limited to Trade Secret and Confidential Information in paper form and in electronic form, wherever and however stored, including but not limited to personal computers, cloud storage, external storage media, smart phones and

other handheld devices, and email accounts) and to the extent that any such information is maintained in electronic form;

3) until further Order of the Court, the Covered Persons are restrained from conducting, carrying on, or engaging in any competitive business that was developed and/or implemented, in whole or in part, directly or indirectly, through the use of any Company Trade Secret and Confidential Information, (the “Prohibited Business”); and

- B. Judgment in favor of Plaintiffs and against Defendant;
- C. An award to Plaintiffs of actual damages (such as lost profits) and disgorgement of amounts by which Defendant has been unjustly enriched, or in the alternative, a reasonable royalty;
- D. An award to Plaintiffs of punitive and/or exemplary damages;
- E. An award to Plaintiffs of their reasonable attorneys’ fees and its costs incurred in this action;
- F. An award to Plaintiffs of pre-judgment and post-judgment interest; and
- G. Such other and further relief as this Court deems just and proper.

Done this 15th day of March 2023.

Respectfully submitted,

/s/ Daniel F. Lanciloti

Daniel F. Lanciloti (admitted *Pro Hac Vice*)
Craig R. Annunziata
James M. Hux, Jr. (admitted *Pro Hac Vice*)
J. Michael Honeycutt (admitted *Pro Hac Vice*)
FISHER PHILLIPS LLP
10 South Wacker Drive
Suite 3450
Chicago, Illinois 60606
Telephone: (312) 346-8061
Facsimile: (312) 346-3179
dlanciloti@fisherphillips.com
cannunziata@fisherphillips.com
jhux@fisherphillips.com
jhoneycutt@fisherphillips.com
ATTORNEY FOR PLAINTIFFS

CERTIFICATE OF SERVICE

I hereby certify that on the 15th day of March 2023 the foregoing document was electronically filed with the Clerk of Court using the CM/ECF system and was served on the following by U.S. mail and e-mail to:

Johanna Wilbert
Quarles & Brady LLP
411 East Wisconsin Avenue, Suite 2400,
Milwaukee, WI 53202-4428
Johanna.Wilbert@quarles.com

Respectfully submitted,

/s/ Daniel F. Lanciloti

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN**

ECOLAB Inc., and NALCO COMPANY,
LLC d/b/a Nalco Water, an Ecolab Company
and/or Nalco Water,

Plaintiffs,

v.

JESSICA GRAILER,


Defendant.

No. 3:23-cv-00102

VERIFICATION

I, Laurence D. Lieb, President of Tyger Forensics Inc., declare under penalty of perjury that the information contained in Paragraphs 36-44, 46-48, 50-54 in the foregoing Verified Complaint is within my personal knowledge and is true and correct.

Executed on March 15, 2023.



Laurence D. Lieb

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN**

ECOLAB Inc., and NALCO COMPANY,
LLC d/b/a Nalco Water, an Ecolab Company
and/or Nalco Water,

Plaintiffs,

v.

JESSICA GRAILER,

Defendant.

No. 3:23-cv-00102

VERIFICATION

I, Corey L. DeMarco, Vice President of NALCO Company LLC d/b/a Nalco Water, an Ecolab Company, declare under penalty of perjury that the information contained in Paragraphs 1-35, 45, 49, and 55-107 in the foregoing Verified Complaint is within my personal knowledge and is true and correct to the best of my knowledge, information, and belief.

Executed on March 14, 2023.



Corey L. DeMarco